КИБЕРБЕЗОПАСНОСТЬ АВТОМАТИЗИРОВАННЫХ СИСТЕМ УПРАВЛЕНИЯ ВОЕННОГО НАЗНАЧЕНИЯ

Зубарев Игорь Витальевич, *кандидат технических наук, доцент*
Жидков Игорь Васильевич, *кандидат технических наук, доцент*
Кадушкин Иван Викторович

Рассмотрены концептуальные вопросы военных информационных операций. Определены цели, задачи, составляющие информационных операций. Проанализированы функциональные и информационных компоненты АСУ военного назначения.

Ключевые слова: *информационная война, информационные операции, кибероперации, АСУ, доктрина информационной безопасности*

THE MILITARY AUTOMATED SYSTEMS CONTROL CYBERSECURITY

Igor Zubarev, Ph.D., *Associate Professor*
Igor Zhidkov, Ph.D., *Associate Professor*
Ivan Kadushkin

The conceptual issues of military information operations are considered. The goals, objectives, components of information operations are identified. The functional and informational components of the military information system are analyzed.

Keywords: *information operations, cyber operations*

При использовании современных информационных технологий (ИТ) в автоматизированных системах управления (АСУ) военного назначения, таких, например, как компьютерные сети и базы данных, ценность информации (с точки зрения решения задач ведения боевых действий) увеличивается, поскольку они дают возможность повысить степень осведомленности, улучшить взаимодействие между командованиями различного уровня, органами военного управления и разведки и, тем самым, реализовать свое информационное превосходство.

С развитием ИТ и с внедрением АСУ, созданных на их основе, а также в связи со стремительным переоснащением войск информационно насыщенным вооружением и военной техникой (ВВТ), высокоточными средствами разведки и поражения и информационного противоборства общепризнанные и традиционные модели управления вооруженными силами начали претерпевать коренные изменения.

На первый план выходят операции, основной составляющей которых является достижение информационного и технологического превосходства. Эти тенденции отчетливо проявились, в частности, в ходе агрессии НАТО на Балканах, в Ираке и Афганистане.

В настоящее время самое пристальное внимание проблеме обеспечения своей кибербезопасности уделяют страны НАТО и КНР. Роль лидера в данной области принадлежит США, которые сформулировали основы стратегии информационного противоборства еще в 1992 году [1-4].

Комитет начальников штабов вооруженных сил США утвердил документ «Информационные операции», в котором излагались взгляды американского военного руководства на их подготовку и проведение, уточнены цели, задачи и основные принципы информационного противоборства, а также обязанности должностных лиц по подготовке и проведению таких операций в мирное и в военное время [10]. Как следовало из документа, информационные операции представляют собой комплекс мероприятий по воздействию на людские и материальные ресурсы противника для того, чтобы затруднить или сделать невозможным

принятие верного решения с одновременной защитой своих информационно-коммуникационных сетей и компьютерных систем. Такие операции включали в себя пять основных составляющих:

- радиоэлектронную борьбу (electronic warfare);
- психологические операции (psychological operations);
- операции в информационно-коммуникационных сетях (computer network operations);
- военную дезинформацию (military deception);
- оперативную безопасность (operations security).

Были определены и вспомогательные элементы информационных операций, необходимые для достижения успеха операции в мирное и в военное время, в том числе:

- информационная устойчивость (information assurance);
- физическое воздействие (physical attack);
- контрразведка (counter intelligence);
- физическая безопасность (physical security);
- сбор и использование данных видовой разведки (combat camera);
- связь с общественностью (public affairs);
- гражданско-военные операции (civil-military operations);
- поддержка структурами минобороны публичной дипломатии (defense support to public diplomacy).

Директива Министерства обороны США D 3600.01 определила основные задачи и функции информационных операций, в целом означающие комплексное применение средств радиоэлектронной борьбы, операций в информационно-коммуникационных сетях, психологических операций, военной дезинформации и оперативной безопасности [8]. В документе отмечалось, что информационные операции проводятся «в целях информационного воздействия, введения в заблуждение, нарушения работы компьютерных систем, искажения информации, дезорганизации баз данных и лишения противника возможности их использования, извлечения информации из компьютерных систем и баз данных противника при одновременном обеспечении защиты своей информации и информационной инфраструктуры». Документ вводил в действие принцип разделения информационных операций на три категории (см. рисунок 1). Подобные директивные документы были изданы всеми видами вооруженных сил [5-11,13].

Рис.1. *Категории информационных операций ВС США*

В 2009 году в США было создано Кибернетическое командование ВС США (USCYBERCOM). При его создании использовалась модель объединенного боевого командования, включающая киберкомандования родов вооруженных сил (рисунок 2). Такая структура, по мнению высшего военного руководства США, позволяет наиболее эффективно задействовать возможности всех видов вооруженных сил США и учитывать их интересы при ведении общевойсковых операций.

Организационно в состав командования входят, кроме центрального подразделения, аналогичные командования сухопутных войск (Cyberspace Task Force), ВВС (AFCOC), ВМС (FLTCYBERCOM), морской пехоты и береговой охраны. Они обеспечивают как защиту собственных компьютерных сетей, так и ведение кибернетических операций в интересах ВС США.

Киберкомандование Сухопутных войск создано в составе Управления по операциям, боеготовности и мобилизации (Directorate of Operations, Readiness and Mobilization - DORM). Как ожидается, в целях расширения возможностей, в него будут переведены профильные подразделения из состава:

- командования космической и противоракетной обороны Стратегического командова-

Рис. 2. *Структура кибернетического командования ВС США*

ния сухопутных войск (Space And Missile Defense Command/Army Forces Strategic Command);

- командования разведки и безопасности армии (Intelligence And Security Command);

- командования развития телекоммуникационных технологий (Network Enterprise Technology Command).

Перед новым подразделением поставлены задачи объединения усилий штаба сухопутных войск (СВ) по управлению информационными системами, разработке политики осуществления операций в киберпространстве, а также утверждению требований и предоставлению ресурсов для создания перспективных тактических и стратегических средств ведения боевых действий в киберпространстве.

В настоящее время Группой по развитию комплексных возможностей (Integrated Capabilities Development Team - ICDT) Командования по боевой подготовке и доктринам сухопутных войск США (TRADOC) разработаны базовые документы, определяющие спектр задач СВ США в киберпространстве на 2010-2024 гг., в частности создана концепция проведения операций с полномасштабным использованием киберсредств Cyber Electronics In Full-Spectrum Operations Concept, а также определены перспективные направления их проведения.

Параллельно над созданием концепции коллективной кибероборонь начали работать и в НАТО. В ноябре 2010 года на саммите альянса было решено разработать «План действий в области кибероборонь». Важное место в нем будет отведено созданию центра НАТО по реагированию на киберинциденты. Изначально его предполагалось запустить в 2015 году, но по настоянию США срок сократили на три года.

В докладе «Возможности КНР вести кибервойну и использовать компьютерные сети», подготовленном в октябре 2009 года для конгресса США группой Northrop Grumman, указывается что в рамках Народно-освободительной армии Китая (НОАК) существует детально разработанная доктрина о применении нападения на компьютерную инфраструктуру противника. Также в НОАК уже созданы специальные подразделения, которые будут производить эти операции в случае военного конфликта. Количество бойцов в них неизвестно, однако, по экспертным оценкам, оно может составлять не менее 30 тыс. человек. Задача по координации наступательных операций в сетевом пространстве возложена на четвертый отдел генштаба НОАК, отвечающий за радиоэлектронную борьбу [5,12].

Для защиты интересов и нейтрализации угроз национальной безопасности в информационной сфере Российской Федерации согласно «Доктрине информационной безопасности Российской Федерации» (№ Пр-1895) создана система обеспечения информационной безопасности государства, в которой Министерство обороны совместно с федеральными органами исполнительной власти и другими государственными органами является одним из основных элементов.

Решая задачи в интересах обеспечения национальной безопасности Российской Федерации, Вооруженные Силы становятся объектом информационных воздействий. В этих условиях Вооруженные Силы должны обеспечивать собственную информационную безопасность на достаточно высоком качественном уровне, которая будет являться залогом успешного решения задач по обеспечению национальной безопасности Российской Федерации.

Таким образом, исходя из взглядов военного руководства иностранных государств и основополагающих принципов применения видов ВС РФ, основанных, прежде всего, на сдерживании возможной агрессии противника, нейтрализация (ослаблении) воздействия противоборствующей стороны на информационные объекты ВС РФ имеет огромнейшее значение.

Виды информационных объектов ВС РФ представлены на рисунке 3.

Рис.3. *Виды информационных объектов ВС РФ*

Хочется отметить, что в настоящее время сетевое противоборство в ВС США выделено в отдельный вид информационного противоборства, который получает приоритетное развитие.

Для этого создается многоуровневая структура сил и средств:

- первый уровень – активные действия против простых сетей;
- второй уровень – проведение «массированных атак» против многоуровневых структурированных систем управления;
- третий уровень – нанесение скоординированных «ударов» по хорошо защищенным криптоустойчивым АСУ.

В таком же направлении совершенствуется система информационного противоборства в вооруженных силах большинства союзников по НАТО, а также в ЕС.

В составе НОАК Китая имеются бригады атак и подразделения защиты информации. Для вывода из строя (нарушения функционирования) критически важных информационных объектов противника НОАК предполагается задействовать большое количество специально подготовленных для этих целей групп.

Несомненно, что операции подразделений кибернетических командований противоборствующей стороны в информационно-коммуникационных сетях будут в первую очередь направлены на информационно-технические объекты ВС РФ. К таковым относятся и АСУ военного назначения.

Таким образом, в связи с прогнозируемым усилением глобального информационного противоборства, активными разработками странами НАТО и КНР средств и методов информационного противоборства, направленных на АСУ военного назначения, обеспечение их кибербезопасности становится одним из приоритетных направлений обеспечения безопасности ВС РФ.

Обеспечение кибербезопасности АСУ военного назначения охватывает мероприятия, направленные на защиту информации, компьютеров и сетей от проникновения, повреждения или уничтожения противником. Наиболее уязвимые элементы инфраструктуры представлены на рисунке 4.

Исходя из рассмотренных аспектов развития сетевого противоборства под ***кибербезопасностью*** АСУ военного назначения следует понимать состояние защищенности хранящейся, обрабатываемой и передаваемой в АСУ военного назначения информации от угроз информационно-технического характера.

Под ***субъектами кибербезопасности*** АСУ военного назначения предлагается понимать органы военного управления высшего звена, видов Вооруженных Сил Российской Федерации, родов войск в части, их касающейся, а также типовые воинские формирования (ТОФ) и их структурные подразделения.

Объектами кибербезопасности АСУ военного назначения (информационными объектами, подлежащими защите от внешних и внутренних угроз) должны являться:

- информационные ресурсы АСУ военного назначения, содержащие сведения, составляющие государственную тайну, а также иную информацию;

Рис. 4. *Элементы инфраструктуры АСУ военного назначения*

- автоматизированные системы, подсистемы и звенья управления высшего звена, видов Вооруженных Сил Российской Федерации, родов войск, а также ТОФ и их структурных подразделений;
- информационно-расчетные системы военного назначения;
- средства вычислительной техники АСУ военного назначения;
- системы, средства связи и телекоммуникации военного назначения;
- информационные и телекоммуникационные технологии;
- технологические процессы;
- технологическая информация и информация управления;
- программное обеспечение (ОС, СУБД, общесистемное и специальное ПО);
- средства зашиты информации;
- средства контроля эффективности СЗИ.

Под угрозой информационно-технического характера АСУ военного назначения предлагается понимать совокупность условий и/или факторов, определяющую информационно-техническое воздействие на информацию и/или состояние АСУ, ее объекты и/или среду функционирования, которые могут привести к недопустимому ущербу или неспособности выполнения АСУ своих функций с требуемым качеством.

При рассмотрении научно-технических проблем обеспечения кибербезопасности АСУ военного назначения целесообразно разделить их внешние и внутренние.

Причиной ***внешних научно-технических проблем обеспечения кибербезопасности АСУ военного назначения*** являются организованные информационно-технические воздействия, проводимые любыми субъектами, находящимися вне юрисдикции Российской Федерации, ведущие к снижению боеготовности ВС РФ. В качестве основных проблем следует отметить:

- разработку рядом стран концепций информационного противоборства, создание ими информационного оружия, а также ведение этими странами различных видов разведки в интересах достижения преимуществ в информационной сфере;
- информационно-технические воздействия на информационные объекты ВС РФ со стороны иностранных государств;
- возрастание технологического отрыва ведущих стран мира, расширяющее зависимость ВС РФ от закупок зарубежной техники для обеспечения функционирования объектов информационной инфраструктуры ВС РФ и увеличивающее возможности зарубежных стран по противодействию созданию отечественных конкурентоспособных современных информационных технологий.

Причиной внутренних научно-технических проблем обеспечения кибербезопасности АСУ военного назначения служат организованные информационно-технические воздействия, проводимые субъектами, находящимися под юрисдикцией Российской Федерации, ведущие к снижению боеготовности ВС РФ.

Таким образом, ***обеспечение кибербезопасности АСУ военного назначения*** должно представлять собой деятельность субъектов информационной безопасности по выявлению и ликвидации (нейтрализации) угроз объектам АСУ военного назначения, снижению рисков и величины возможного ущерба.

При этом основными задачами обеспечения кибербезопасности АСУ военного назначения должны являться:

- систематическое выявление и устранение угроз кибербезопасности АСУ военного назначения и их источников;

- развитие и совершенствование системы обеспечения кибербезопасности АСУ военного назначения, реализующей единую государственную политику в этой области, включая разработку новых и совершенствование существующих способов, методов и средств выявления, оценки, прогнозирования, нейтрализации и ликвидации угроз, а также средств и методов противодействия этим угрозам;

- эффективное противодействие угрозам кибербезопасности АСУ военного назначения;

- разработка основных направлений военно-технической политики в области обеспечения кибербезопасности АСУ военного назначения, а также мероприятий и механизмов, связанных с реализацией этой политики;

- разработка критериев и методов оценки эффективности системы обеспечения кибербезопасности АСУ военного назначения;

- совершенствование нормативно-правовой базы по обеспечению кибербезопасности АСУ военного назначения;

- координация деятельности органов военного управления в области обеспечения кибербезопасности АСУ военного назначения;

- разработка научно-практических основ обеспечения кибербезопасности АСУ военного назначения;

- разработка и реализация целевых программ, направленных на обеспечение кибербезопасности АСУ военного назначения;

- создание базовых информационных защищенных компьютерных технологий;

- выявление, предотвращение и ликвидация последствий информационных воздействий, вызывающих утечку, перехват, уничтожение, искажение информации или сбои в работе АСУ военного назначения;

- организация и обеспечение защиты информации с использованием средств защиты информации, в том числе криптографических;

- совершенствование системы сертификации средств защиты информации Министерства обороны по требованиям безопасности информации;

- сертификация средств защиты информации, программного обеспечения, технологий их разработки и применения в соответствии с требованиями информационной безопасности;

- совершенствование приемов, способов, методов и средств защиты АСУ военного назначения от информационно-технических воздействий противоборствующей сторны;

- совершенствование системы подготовки кадров.

При выполнении указанных задач необходимо руководствоваться следующими основными принципами системной инженерии:

- **достаточность** – соответствие уровня затрат (комплекса мероприятий) на обеспечение кибербезопасности величине возможного ущерба АСУ военного назначения;

- **комплексность** – комплексное использование разнородных способов, методов и средств обеспечения кибербезопасности АСУ военного назначения;

- **непрерывность** – способность системы обеспечения кибербезопасности АСУ военного назначения обеспечивать их защищенность в любых условиях;

- **оперативность** – своевременное реагирование на изменение условий и факторов, создающих угрозы АСУ военного назначения;

- **системность** – осуществление системного подхода к обеспечения кибербезопасности АСУ военного назначения;

- **целенаправленность** – строгое подчинение целей и задач мероприятий по достижению требуемого уровня защищенности АСУ военного назначения общему замыслу обеспечения информационной безопасности ВС РФ.

ВЫВОДЫ

Деятельность по совершенствованию системы обеспечения киберезопасности АСУ военного назначения должна базироваться на результатах глубокого научного предварительного анализа состояния правовых, организационных, технических и экономических основ системы. Должно быть проведено изучение и обобщение зарубежного опыта и опыта деятельности по этим вопросам других государственных структур. Первоочередными в этой работе должны быть следующие мероприятия:

- развитие научно-практических основ кибербезопасности АСУ военного назначения;

- дальнейшее совершенствование и развитие нормативной и правовой базы обеспечения кибербезопасности АСУ военного назначения;

- развитие современных способов, методов и средств обеспечения кибербезопасности АСУ военного назначения, в т.ч. на основе программных или аппаратно-программных решений из состава системы предупреждения и обнаружения компьютерных атак;

- совершенствование организационно-штатной структуры системы кибербезопасности АСУ военного назначения;

- развитие системы подготовки специалистов в области обеспечения кибербезопасности АСУ военного назначения.

Литература

1. Бобров А. Информационная война: от листовки до твиттера // Зарубежное военное обозрение. 2013. №1. С. 20-27.
2. Корсаков Г.Б. Роль информационного оружия в военно-политической стратегии США // США и Канада: экономика, политика, культура. 2012. № 1. С. 39-60.
3. Пашков В. Информационная безопасность США // Зарубежное военное обозрение. 2010. №10. С.3-13.
4. Роговский Е.А. Политика США по обеспечению безопасности киберпространства // США и Канада: экономика, политика, культура. 2012. № 6. С. 3-22.
5. Храмчихин А.А. Стратегические концепции Китая в геополитическом аспекте // Международные научные исследования. 2011. № 3-4. С. 18-23.
6. AFDD 3-12. Cyberspace Operations USAF 2010 60 p.
7. AFDD 3-13. Information Operations USAF 2011 65 p.
8. AFPD 10-7. Information Operations. USAF. 2006. 29 p.
9. DoDD 3600.1. Information Operations. US DoD. 2013. 12 p.
10. Information Operations Primer: Fundamentals of Information Operations. U.S. Army War College, 2011. 204 p.
11. JP 3-13. Information Operations. US Joint Chiefs of Staff, 2012. 69 p.
12. JP 3-13.1. Electronic Warfare. US Joint Chiefs of Staff, 2007. 115 p.
13. Vinod A. Chinese Concepts and Capabilities of Information Warfare // Strategic Analysis. 2006. Vol. 30. No. 4. P. 781-797.
14. Wade N.M. The Joint Forces Operations & Doctrine. The Lightning Press, 2012. 75 p.

References

1. Bobrov A. Informatsionnaya voyna: ot listovki do tvittera, (Information Warfare : from flyers twitter) Zarubezhnoye voyennoye obozreniye, 2013, No 1, pp. 20-27.
2. Korsakov G.B. Rol informatsionnogo oruzhiya v voyenno-politicheskoy strategii USA, (The role of information warfare in military and political strategy of the United States), SShA i Kanada: ekonomika, politika, kultura, 2012. No 1, pp. 39-60.
3. Pashkov V. Informatsionnaya bezopasnost USA (US Information Security), Zarubezhnoye voyennoye obozreniye, 2010, No 10, pp. 3-13.
4. Rogovskiy Ye.A. Politika SShA po obespecheniyu bezopasnosti kiberprostranstva, (Policy to Secure Cyberspace), SShA i Kanada: ekonomika, politika, kultura, 2012, No 6, pp. 3-22.
5. Khramchikhin A.A. Strategicheskiye kontseptsii Kitaya v geopoliticheskom aspekte, (The strategic concept of China 's geopolitical aspect), Mezhdunarodnyye nauchnyye issledovaniya, 2011, No 3-4, pp. 18-23.
6. AFDD 3-12. Cyberspace Operations USAF 2010 60 p.
7. AFDD 3-13. Information Operations USAF 2011 65 p.
8. AFPD 10-7. Information Operations. USAF. 2006. 29 p.
9. DoDD 3600.1. Information Operations. US DoD. 2013. 12 p.
10. Information Operations Primer: Fundamentals of Information Operations. U.S. Army War College, 2011. 204 p.
11. JP 3-13. Information Operations. US Joint Chiefs of Staff, 2012. 69 p.
12. JP 3-13.1. Electronic Warfare. US Joint Chiefs of Staff, 2007. 115 p.
13. Vinod A. Chinese Concepts and Capabilities of Information Warfare // Strategic Analysis. 2006. Vol. 30. No. 4. P. 781-797.
14. Wade N.M. The Joint Forces Operations & Doctrine. The Lightning Press, 2012. 75 p.